

Hearing Date: 1/4/2023 9:30 AM
 Location: Court Room 2308
 Judge: Cohen, Neil J

12-Person Jury

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
 COUNTY DEPARTMENT, CHANCERY DIVISION**

JOHN BENNETT,
 Individually and on behalf of all others
 similarly situated,

Plaintiff,

v.

**SAMSUNG ELECTRONICS
 AMERICA, INC.**

Defendant.

Case No.:

Hon.

2022CH08767

Calendar

Courtroom

FILED
 9/2/2022 8:06 PM
 IRIS Y. MARTINEZ
 CIRCUIT CLERK
 COOK COUNTY, IL
 2022CH08767
 Calendar, 5
 19357984

FILED DATE: 9/2/2022 8:06 PM 2022CH08767

CLASS ACTION COMPLAINT

Plaintiff John Bennett, individually and on behalf of all others similarly situated, brings this Class Action Complaint and Demand for Jury Trial against Defendant Samsung Electronics America, Inc. ("Samsung"), to seek redress for Samsung's conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of millions of its customers. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

NATURE OF THE CASE

1. Defendant Samsung Electronics America, Inc. ("Samsung") or ("Defendant") failed to safeguard the confidential personal identifying information of Plaintiff John Bennett ("Plaintiff") and millions of individuals ("Class Members" or collectively as the "Class"). This class action is brought on behalf of Class Members whose personally identifiable information ("PII" or "Private Information") was stolen

by cybercriminals in a cyber-attack that accessed sensitive patient information through Defendant's email accounts.

2. In July 2022 Defendant lost valuable PII regarding its customers due to unauthorized access from cybercriminals.

3. Defendant became aware of this breach on or about August 4, 2022, but waited until September 2, 2022, to inform its customers that their PII had been compromised.

4. Plaintiff and Class Members were not notified of the data breach until September 2022, more than a month after their information was first accessed.

5. The cybercriminals accessed insufficiently protected information belonging to Plaintiff and the Class Members. Upon information and belief, as a result of Defendant's failure to properly secure Plaintiff's and the Class Members' personal information, the cybercriminals obtained extensive personal information including names, contact and demographic information, dates of birth, and product registration information, collectively known as personally identifiable information ("PII" or "Private Information").

6. Plaintiff's and Class Members' sensitive personal information, which was entrusted to Defendant, its officials and agents, was compromised, unlawfully accessed, and stolen due to the data breach.

7. As a result of Defendant's actions and/or inaction, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all Class Members are currently at a very high

risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized account access including on third-party services and identity theft through use of personal information to open up accounts.

8. Defendant's wrongful actions and/or inaction constitute Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), common law negligence, invasion of privacy by the public disclosure of private facts, breach of contract, and breach of implied contract.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

10. Plaintiff, on behalf of himself and the Class seeks (i) actual damages, economic damages, emotional distress damages, statutory damages and/or nominal damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

JURISDICTION AND VENUE

11. Jurisdiction over Defendant is proper under 735 ILCS 5/2-209(a)(1) (transaction of any business within this State), section 2-209(b)(4) (corporation doing business within this State), and section 2-209(c) (any other basis now or hereafter permitted by the Illinois Constitution and the Constitution of the United States).

FILED DATE: 9/2/2022 8:06 PM 2022CH08767

12. Venue is proper in this county pursuant to 735 ILCS 5/2-101, because this is the county in which the transactions and occurrences at issue, or some part thereof, occurred. In addition, Defendant regularly do business in this county. 735 ILCS 5/2-102(a).

13. Pursuant to General Order No. 1.2 of the Circuit Court of Cook County, this action is properly before the Chancery Division of the County Department because it is a putative Class Action.

PARTIES

14. Plaintiff John Bennett was a resident and citizen of the State of Illinois during all times relevant to this complaint.

15. Defendant Samsung Electronics America, Inc., is a New York based corporation that does business internationally and within all 50 states, including Illinois.

FACTUAL ALLEGATIONS

16. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

17. According to the Federal Trade Commission ("FTC"):

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or

cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

18. The United States Government Accountability Office (“GAO”) has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person’s name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim’s credit rating. Like the FTC, the GAO explained that victims of identity theft face “substantial costs and inconvenience repairing damage to their credit records” as well the damage to their “good name.”

19. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization’s cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

20. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

21. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed by Defendant.

22. The FTC has issued a publication entitled “Protecting Personal Information: A Guide for Business” (“FTC Report”). The FTC Report provides guidelines for businesses on how to develop a “sound data security plan” to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

- a. Know what personal information you have in your files and on your computers;
- b. Keep only what you need for your business;
- c. Protect the information that you keep;
- d. Properly dispose of what you no longer need;
- e. Control access to sensitive information by requiring that employees use “strong” passwords; tech security experts believe the longer the password, the better; and
- f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

23. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

24. The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

25. Upon information and belief, Defendant has policies and procedures in place regarding the safeguarding of confidential information they are entrusted with and Defendant failed to comply with those policies. Defendant also negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiffs and the Class’ confidential information being substantially less safe than had this information been entrusted with other similar companies.

26. On or around September 2, 2022, Plaintiff and millions of Class Members received emailed letters from Defendant notifying them that Defendant learned of suspicious activity that allowed one or more cybercriminals to access their systems containing Plaintiffs and the Class’ Personally Identifiable Information.

27. The criminals were able to access Plaintiffs and the Class’ personal information because Defendant failed to take reasonable measures to protect the Personally Identifiable Information they collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this

attack, despite repeated industry wide warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

28. Defendant's notice of data breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed their accounts, whether the information was encrypted or otherwise protected, how they learned of the data breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many individuals were affected by the data breach.

29. As a result of Defendant's failure to properly secure Plaintiff's and the Class Members' personal identifying information, Plaintiff's and the Class Members' privacy has been invaded.

30. Defendant also refused to provide credit monitoring or other services to assist Plaintiff and the class members' in monitoring their credit to help avoid identity theft.

31. Moreover, all of this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and the Class Members' unencrypted, non-redacted information, including names, addresses, email addresses, phone numbers and social security numbers, and other potential PII.

32. As a direct and proximate result of Defendant's wrongful disclosure, criminals now have Plaintiff's and the Class Members' personal identifying information. Additionally, the disclosure makes Plaintiff and Class Members much

more likely to respond to requests from Defendant or law enforcement agencies for more personal information, such as bank account numbers, login information or even Social Security numbers. Because criminals know this and are capable of posing as Defendant or law enforcement agencies, consumers like Plaintiff and fellow Class Members are more likely to unknowingly give away their sensitive personal information to other criminals.

33. Defendant's wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendant's wrongful actions and/or inaction, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

34. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

35. Defendant's wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendant's wrongful actions and/or inaction,

Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

36. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

37. The PII included in the data breach, combined with other contact information which can be obtained from other sources, is very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the data breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

38. As a direct and proximate result of the data breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received

as a result of the data breach. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to and misuse of their Private Information from Defendant. Plaintiff and Class Members presently and will continue to suffer from damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

39. Defendant was at all times fully aware of its obligations to protect the Private Information of Plaintiff and Class Members. Plaintiff and Class Members would not have entrusted their Private Information to Defendant had they known that Defendant would fail to maintain adequate data security. Defendant was also aware of the significant repercussions that would result from their failure to do so.

40. While this matter has only recently been discovered, Plaintiff believes that through discovery additional information will be obtained including what additional information may have been compromised by Defendant's actions and inactions, what actions Defendant took or did not take to secure data, and other information regarding the data breach.

41. Accordingly, Plaintiff on behalf of himself and the Class, brings this action against Defendant seeking redress for their unlawful conduct.

CLASS ALLEGATIONS

42. Plaintiff brings these claims on behalf of the following classes:

National Class: All individuals whose PII was disclosed while in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Breach.

Illinois Sub-Class: All individuals in Illinois whose PII was disclosed while in the possession of Defendant, or any of their subsidiaries and/or agents, during the Data Breach.

43. Plaintiff may alter the class definitions to conform to developments in the case and discovery.

44. The proposed classes meet all requirements under 735 ILCS 5/2-801.

45. The putative Classes are comprised of thousands of persons, making joinder impracticable. The joinder of the Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the Court. The Classes can be identified through Defendant's records or Defendant's agents' records.

46. The rights of each Class Member were violated in an identical manner as a result of Defendant's willful, reckless and/or negligent actions and/or inaction.

47. **Numerosity:** Upon information and belief, the Classes are so numerous that joinder of all individual plaintiffs would be impracticable. The exact number of members of the Classes are presently unknown and can only be ascertained through discovery because that information is exclusively in the possession of the Defendant. However, it is reasonable to infer that more than 40 individuals in each class were impacted by the data breach at issue. Members of the Classes can be easily identified through Defendant's records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may

include U.S. mail, electronic mail, Internet postings, and/or published notice.

48. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Classes, including, without limitation:

- a. Whether Defendant negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs and Class Members' personal identifying information;
- b. Whether Defendant was negligent in storing and failing to adequately safeguard Plaintiffs and Class Members' personal identifying information;
- c. Whether Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their personal identifying information;
- d. Whether Defendant breached its duties to exercise reasonable care in failing to protect and secure Plaintiffs and Class Members' personal identifying information;
- e. Whether by disclosing Plaintiffs and Class Members' personal identifying information without authorization, Defendant invaded Plaintiffs and Class Members' privacy;
- f. Whether Defendant created an implied contract with Plaintiff and Class Members to keep their personal identifying information confidential; and
- g. Whether Plaintiff and Class Members sustained damages as a result of Defendant's failure to secure and protect their personal identifying information.

49. **Adequacy of Representation:** Plaintiff is an adequate representative of the Classes because his interests do not conflict with the interests of the

members of the Classes he seeks to represent and he intends to prosecute this action vigorously. Plaintiff has retained counsel competent and experienced in consumer class actions and complex litigation. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel and Plaintiff's claim is typical of the claims of the class members.

50. **Appropriateness:** A class action in this case would be appropriate and superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Classes are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Classes to individually seek redress for Defendant's wrongful conduct. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the judicial system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

51. Defendant has acted or failed to act on grounds that apply generally to the class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

**COUNT I - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND
DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, ET SEQ.**

(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

52. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

53. Section 2 of the Illinois Consumer Fraud Act (ICFA) prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the “Uniform Deceptive Trade Practices Act”, approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

54. Defendant violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff.

55. Specifically, it was an unfair act and practice to represent to Plaintiff and the Illinois Subclass members that it implemented commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations, including by failing to timely detect the Data Vulnerability.

56. Despite representing to Plaintiff and the Illinois Subclass members that it would implement commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations.

57. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant’s unlawful conduct and violations of the ICFA and analogous state statutes.

58. Defendant's conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers PII.

59. An award of punitive damages is appropriate because Defendant's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of the Plaintiff and consumers, generally, and Plaintiff had no choice but to submit to Defendant's illegal conduct.

COUNT II - NEGLIGENCE

(ON BEHALF OF PLAINTIFF AND THE CLASS)

60. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

61. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

62. Defendant owed a duty of care not to subject Plaintiff's and the Class' Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

63. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members'

personal identifying information would result in an unauthorized third-party gaining access to such information for no lawful purpose, and that such third parties would use Plaintiff's and Class Members' personal identifying information for malevolent and unlawful purposes, including the commission of direct theft and identity theft.

64. Defendant knew, or should have known, of the risks inherent in collecting, storing, and sharing Private Information amongst themselves and the importance of adequate security. Defendant knew of should have known about numerous well-publicized data breaches within the industry.

65. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they suffered loss and are entitled to compensation.

66. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, negligence at common law.

COUNT III - INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE

FACTS AND INTRUSION UPON SECLUSION

(ON BEHALF OF PLAINTIFF AND THE CLASS)

67. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

68. Plaintiff's and Class Members' Personal Identifying Information is and always has been private information.

69. Dissemination of Plaintiff's and Class Members' private information is not of a legitimate public concern; publication to third parties of their personal identifying information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

70. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they are entitled to compensation.

71. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their personal identifying information).

COUNT IV - BREACH OF CONTRACT

72. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

73. Plaintiff and other Class Members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class Members agreed to provide their Private Information to Defendant, and Defendant impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

74. To the extent Defendant's obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with FCC regulations; federal, state and local laws; and industry standards. Neither Plaintiff nor any Class member would have entered into these contracts with Defendant without the understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

75. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

76. The protection of Plaintiff's and Class Members' Private Information was a material aspect of Plaintiff's and Class Members' contracts with Defendant.

77. Defendant's promises and representations described above relating to FCC regulations and industry practices, and Defendant's purported concern about its clients' privacy rights became terms of Plaintiff's and Class Members' contracts with

Defendant. Defendant breached these promises by failing to comply with FCC regulations and reasonable industry practices.

78. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect their Private Information if that information was provided to Defendant.

79. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

80. As a result of Defendant's breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the lost difference in the value between the secure services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the data breach on their lives, including, inter alia, to close or modify financial and medical accounts, and to closely review and monitor credit reports and various accounts for unauthorized activity. Additionally, Plaintiff and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

81. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and fees and costs of litigation.

COUNT V - BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

(IN ALTERNATIVE TO COUNT IV)

82. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

83. At all relevant times, Defendant had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of Plaintiff and the Class members, and to prevent the unauthorized access to and disclosures of this data.

84. Among other things, Plaintiff and Class Members were required to disclose their personal identifying information to Defendant for the provision of services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

85. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

86. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

87. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to protect Plaintiffs and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

88. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's data breach notification letters and Defendant's notices of privacy practices.

89. Defendant's express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

90. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendant's goods and/or services.

91. Defendant materially breached its contractual obligations to protect the private information Defendant gathered when the information was accessed and exfiltrated during the data breach.

92. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy

practices. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notification of the data breach to Plaintiff and Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' private information as set forth above.

93. The data breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

94. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the secure services Defendant promised and the insecure services received.

95. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with Defendant.

96. As a direct and proximate result of the data breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of

suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff asks for an award in his favor and against Defendant as follows:

- A. Certifying this action as a class action, with a class as defined above;
- B. Designation of Plaintiff as representative of the proposed Class and designation of Plaintiff's counsel as Class counsel;
- C. For equitable relief enjoining Defendant from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- D. Awarding compensatory damages to redress the harm caused to Plaintiff and Class Members in the form of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm. Plaintiff and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and Class Members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court.
- E. Ordering injunctive relief including, without limitation, (i) adequate credit monitoring, (ii) adequate identity theft insurance, (iii) instituting security

protocols in compliance with the appropriate standards and (iv) requiring Defendant to submit to periodic compliance audits by a third party regarding the security of personal identifying information in its possession, custody and control.

F. Awarding Plaintiff and the Class Members interest, costs and attorneys' fees;

G. Compensatory damages, punitive damages and attorneys' fees and the costs of this action as allowed under the Illinois Consumer Fraud Act; and

H. Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

Respectfully Submitted,

By: /s/ Bryan Paul Thompson
One of Plaintiff's Attorneys

Bryan Paul Thompson
Robert W. Harrer
CHICAGO CONSUMER LAW CENTER, P.C.
Cook County Firm No. 62709
33 N. Dearborn St., Suite 400
Chicago, Illinois 60602
Tel. 312-858-3239
Fax 312-610-5646
bryan.thompson@cclc-law.com
rob.harrer@cclc-law.com

Michael Kind, Esq. (*Pro Hac Vice* Forthcoming)
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Phone: (702) 337-2322
FAX: (702) 329-5881
Email: mk@kindlaw.com